ISBN : 978-602-9494-97-6

Intrusion Detection with On – line Clustering Using Reinforcement Learning

Indah Yulia Prafitaning Tiyas, Ali Ridho Barakbah, Tri Harsono, Amang Sudarsono
Postgraduate Applied Engineering of Technology
Division of Information and Computer Engineering, Department of Information and Computer Engineering, Electronic Engineering Polytechnic Institute of Surabaya (EEPIS)
EEPIS Campus, Jalan Raya ITS, Sukolilo 60111, Indonesia
Telp :+62(31)5947280, Fax:+62(31)5946114
indahyuliap@yahoo.com, ridho@eepis-its.edu, trison@eepis-its.edu, amang@eepis-its.edu

Abstract

Today, information technology is growing rapidly, we can obtain all the information much easier. Almost all the important information can be accessed by the users. These conditions raise some new problems, one of them is unauthorized access to the system. We need a reliable network security system that is resistant to a variety of attacks against the system. Therefore, Intrusion Detection System (IDS) required to overcome the problems of intrusions. Many researches have been done on intrusion detection using classification methods. Classification method has high precision, but to get a high precision required a determination of the proper classification model. In this paper, we propose a new approach to detect intrusion with On-line Clustering using Reinforcement Learning. Based on the experimental result, our proposed technique can detect intrusions with high accuracy (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R) and high speed (65 ms).

Keywords: Intrusion Detection System, On-Line Clustering, Reinforcement Learning, Unsupervised Learning.

1. Introduction

Based on data compiled by the CERT [8], the number of intrusions from year to year is increase. From 1995 to 2008, the total attack as summarized by CERT is 46.156, as illustrated in figure 1:

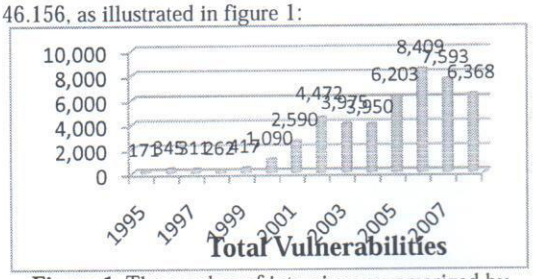

Figure 1. The number of intrusions summarized by CERT[8]

Meanwhile, according to data analyzed by Carnegie Mellon University (2002) and Idaho National Laboratory (2005), intruder technical knowledge decreases, as illustrated in figure 2:

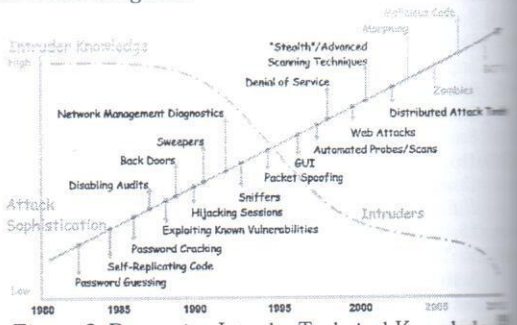

Figure 2. Decreasing Intruder Technical Knowledge

Therefore, Intrusion Detection System (IDS) required to overcome the problems of intrusion. The system that detects and logs illegal access is called an intrusion detection system [1]. There are three categories of intrusion detection systems which are host-based where information is found on a single or multiple host systems, network- based that examines the information captured from network communications and vulnerability assessment-based that identifies vulnerabilities in internal networks and firewall, whereas based on the functionality intrusion detection can be classified into two as anomaly detection and misuse detection [1].

Misuse detection is a system that works by comparing the packet traffic on the computer network with signature database. The weakness of misuse detection is not able to detect any new attacks because the attack was not found in the signature database so that late in detecting the attack. In addition, the administrator must manually update signature database. Anomaly detection is a system that comparing the packet traffic on the computer network with a normal traffic pattern, but it has the disadvantage of sending a lot